Certified Cisco Networking Associate v1.1 (640-802)

Exam Description: The "Cisco Certified Networking Associate" v1.1 640-802 is the composite exam that is associated with Cisco CCNA® Routing and Switching certification. The 640-802 is a 1.5-hour exam with 45–55 questions. Candidates can prepare for this exam by taking the "Interconnecting Cisco Networking Devices: Accelerated" (CCNAX) v1.1 course. This exam tests a candidate's knowledge and skills required to install, operate, and troubleshoot a small to medium-size enterprise branch network. The topics include connecting to a WAN, implementing network security, network types, network media, routing and switching fundamentals, the TCP/IP and OSI models, IP addressing, WAN technologies, operating and configuring IOS devices, extending switched networks with VLANs, determining IP routes, managing IP traffic with access lists, establishing point-to-point connections, and establishing Frame Relay connections.

The following topics are general guidelines for the content that is likely to be included on the exam. However, other related topics may also appear on any specific instance of the exam. To better reflect the contents of the exam and for clarity purposes, these guidelines may change at any time without notice.

15% 1.0 Describe the Operation of Data Networks

1.1 Describe the purpose and functions of various network devices

1.2 Select the components required to meet a given network specification

1.3 Use the OSI and TCP/IP models and their associated protocols to explain how data flows in a network

1.4 Describe common networking applications including web applications

1.5 Describe the purpose and basic operation of the protocols in the OSI and TCP models

1.6 Describe the impact of applications (VoIP and video over IP) on a network

1.7 Interpret network diagrams

1.8 Determine the path between two hosts across a network

1.9 Describe the components required for network and Internet communications

1.10 Identify and correct common network problems at Layers 1, 2, 3, and 7 using a layered model approach

1.11 Differentiate between LAN and WAN operation and features

26% 2.0 Implement a Small Switched Network (26%)

2.1 Select the appropriate media, cables, ports, and connectors to connect switches to other network devices and hosts

2.2 Explain the technology and media access control method for Ethernet technologies

2.3 Explain network segmentation and basic traffic management concepts

2.4 Explain the operation of Cisco switches and basic switching concepts

2.5 Perform, save, and verify initial switch configuration tasks including remote access management

2.6 Verify network status and switch operation using basic utilities
- 2.6.a ping
- 2.6.b traceroute
- 2.6.c telnet
- 2.6.d SSH
- 2.6.e arp
- 2.6.f ipconfig
- 2.6.g Show and debug commands

2.7 Implement and verify basic security for a switch
- 2.7.a Port security
- 2.7.b Deactivate ports
- 2.7.c Trunk access
- 2.7.d Management VLAN other than VLAN 1

2.8 Identify, prescribe, and resolve common switched network media issues
- 2.8.a Configuration issues
- 2.8.b Auto-negotiation
- 2.8.c Switch hardware failures

2.9 Describe enhanced switching technologies.
- 2.9.a VTP
- 2.9.b RSTP
- 2.9.c VLAN
- 2.9.d PVSTP
- 2.9.e 802.1q

2.10 Describe how VLANs create logically separate networks and the need for routing between them

2.11 Configure, verify, and troubleshoot VLANs

2.12 Configure, verify, and troubleshoot trunking on Cisco switches

2.13 Configure, verify, and troubleshoot inter-VLAN routing

2.14 Configure, verify, and troubleshoot VTP

2.15 Configure, verify, and troubleshoot RSTP operation

2.16 Interpret the output of various show and debug commands to verify the operational status of a Cisco switched network

11% 3.0 Implement an IP Addressing Scheme and IP Services to Meet Network Requirements for a Small Branch Office

3.1 Describe the need and role of addressing in a network

3.2 Create and apply an addressing scheme to a network

3.3 Assign and verify valid IP addresses to hosts, servers, and networking devices in a LAN environment

3.4 Explain the basic uses and operation of NAT in a small network connecting to one ISP

3.5 Describe and verify DNS operation

3.6 Describe the operation and benefits of using private and public IP addressing

3.7 Enable NAT for a small network with a single ISP and connection using SDM and verify operation using CLI commands

3.8 Configure, verify, and troubleshoot DHCP and DNS operation on a router (CLI and SDM)

3.9 Implement static and dynamic addressing services for hosts in a LAN environment

3.10 Identify and correct IP addressing issues

3.11 Calculate and apply a VLSM IP addressing design to a network

3.12 Determine the appropriate classless addressing scheme using VLSM and summarization to satisfy addressing requirements in a LAN/WAN environment

3.13 Describe the technological requirements for running IPv6
- 3.13.a Protocols
- 3.13.b Dual stack
- 3.13.c Tunneling

3.14 Describe IPv6 addresses

3.15 Identify and correct common problems associated with IP addressing and host configurations

30% **4.0** **Configure and Troubleshoot [gh1]Basic Operation and Routing on Cisco Devices**

4.1 Compare and contrast methods of routing and routing protocols.

4.2 Configure, verify, and troubleshoot OSPF.

4.3 Configure, verify, and troubleshoot EIGRP.

4.4 Verify configuration and connectivity using basic utilities:
- 4.4.a ping
- 4.4.b traceroute
- 4.4.c telnet
- 4.4.d ssh

4.5 Troubleshoot routing implementation issues.

4.6 Verify router hardware and software operation using show and debug commands.

4.7 Implement basic router security.

25% **5.0** **Implement a Small Routed Network**

5.1 Describe basic routing concepts.
- 5.1.a Packet forwarding
- 5.1.b Router lookup process

5.2 Describe the operation of Cisco routers.
- 5.2.a Router bootup process
- 5.2.b POST
- 5.2.c Router components

5.3 Select the appropriate media, cables, ports, and connectors to connect routers to other network devices and hosts.

5.4 Configure, verify, and troubleshoot RIPv2.

5.5 Access and utilize the router CLI to set basic parameters.

5.6 Connect, configure, and verify operation status of a device interface

5.7 Verify device configuration and network connectivity using basic utilities:
- 5.7.a ping
- 5.7.b traceroute
- 5.7.c telnet
- 5.7.d SSH
- 5.7.e other utilities

5.8 Perform and verify routing configuration tasks for a static or default route given specific routing requirements.

5.9 Manage IOS configuration files.
- 5.9.a save
- 5.9.b edit
- 5.9.c upgrade
- 5.9.d restore

5.10 Manage Cisco IOS.

5.11 Implement password and physical security.

5.12 Verify network status and router operation using basic utilities:
- 5.12.a ping
- 5.12.b traceroute
- 5.12.c telnet
- 5.12.d ssh
- 5.12.e arp
- 5.12.f ipconfig
- 5.12.g show and debug commands

5.13 Compare and contrast methods of routing and routing protocols.

5.14 Configure, verify, and troubleshoot OSPF.

5.15 Configure, verify, and troubleshoot EIGRP.

5.16 Verify configuration and connectivity using basic utilities:
- 5.16.a ping
- 5.16.b traceroute
- 5.16.c telnet
- 5.16.d ssh

5.17 Troubleshoot routing implementation issues

5.13 Verify router hardware and software operation using show and debug commands.

5.14 Implement basic router security.

2% 6.0 Explain and Select the Appropriate Administrative Tasks Required for a WLAN (2%)

6.1 Describe the standards associated with wireless media.
- 6.1.a IEEE WI-FI Alliance
- 6.1.b ITU/FCC

6.2 Identify and describe the purpose of the components in a small wireless network.
- 6.2.a SSID
- 6.2.b BSS
- 6.2.c ESS

6.3 Identify the basic parameters to configure on a wireless network to ensure that devices connect to the correct access point.

6.4 Compare and contrast wireless security features and capabilities of WPA security.
- 6.4.a Open
- 6.4.b WEP
- 6.4.c WPA-1/2

6.5 Identify common issues associated with implementing wireless networks.

6% 7.0 Identify Security Threats to a Network and Describe General Methods to Mitigate Those Threats

7.1 Explain today's increasing network security threats and the need to implement a comprehensive security policy to mitigate the threats.

7.2 Explain general methods to mitigate common security threats to network devices, hosts, and applications.

7.3 Describe the functions of common security appliances and applications.

7.4 Describe recommended security practices including initial steps to secure network devices.

9% 8.0 Implement, Verify, and Troubleshoot NAT and ACLs in a Medium-Size Enterprise Branch Office Network

8.1 Describe the purpose and types of access control lists.

8.2 Configure and apply access control lists based on network filtering requirements.

8.3 Configure and apply an access control list to limit Telnet and or SSH access to the router.

8.4 Verify and monitor ACLs in a network environment.

8.5 Troubleshoot ACL implementation issues.

8.6 Explain the basic operation of NAT.

8.7 Configure NAT for given network requirements using the CLI.

8.8 Troubleshoot NAT implementation issues.

6% 9.0 Implement and Verify WAN Links

9.1 Describe different methods for connecting to a WAN.

9.2 Configure and verify a basic WAN serial connection.

9.3 Configure and verify Frame Relay on Cisco routers.

9.4 Troubleshoot WAN implementation issues.

9.5 Describe VPN technology.
- 9.5.a Importance
- 9.5.b Benefits
- 9.5.c Role
- 9.5.d Impact
- 9.5.e Components

9.6 Configure and verify PPP connection between Cisco routers.